REMARKS

Reconsideration of the application is requested.

Claims 1-13 remain in the application. Claims 1-13 are subject to examination. Claim 9 has been amended.

Under the heading "Drawings" on page 1 of the above-identified Office Action, the Examiner objected to the drawings because they allegedly are not shown with suitable descriptive legends. Figs. 1-3 are flow charts and do not need descriptive legends. In Fig. 4 every box appears to be labeled with a legend. Applicants respectfully request that the Examiner review her comments and if she still believes that the drawings are missing proper legends to be more specific and identify the figure and related box(es) which she feels have inappropriate legends.

Under the heading "Claim Objections" on page 3 of the above-identified Office Action, claim 9 has been rejected as being incomprehensible. More specifically, the Examiner states that line 11 is incomprehensible. Applicants agree and claim 9 has been amended accordingly.

Under the heading "Claim Rejections - 35 USC § 103" on pages 3-7 of the above-identified Office Action, claims 1-13 have been rejected as being obvious over the article entitled "Efficient Elliptic Curve Exponential" by Miyaji et al. (hereinafter Miyaji) in view of the article entitled "Elliptic Curve Cryptosystems" by Menezes (hereinafter Menezes) under 35 U.S.C. § 103.

The invention of the instant application concerns a method of cryptographic processing on a computer, in which an elliptic curve in a first form $y^2 = x^3 + ax + b$ is transformed into an elliptic curve in a second form, $y^2 = x^3 + c^4ax + c^6b$. The purpose of the transformation is to reduce the length of the parameters used for describing the elliptic curve and thus to save memory space in applications with very small memory, such as smart cards. The invention of the instant application describes how the parameter "c" is to be selected so that at least the length of the parameter "a" is significantly reduced.

In Miyaji both the first form and the second form of the elliptic curve are given on page 3. The second form is obtained by transforming the first form by using so-called Jacobian coordinates. The reason given by Miyaji for using Jacobian coordinates is that the required computation amount can be reduced. In Jacobian coordinates a curve doubling requires less computation, while a curve addition requires more computation amount than in the original coordinates. Jacobian coordinates are thus especially suitable for elliptic curve exponentiation since in elliptic curve exponentiation the number of curve additions required can be reduced by a suitable algorithm, but that of curve doublings may not be reduced. Table 1 on page 3 compares the computation amount for curve addition and curve doubling in the original coordinates and in Jacobean coordinates.

In contrast to the invention, no mention of the length of the parameters of the elliptic curves is made by Miyaji. The second form of the elliptic curves is used only for the purpose of reducing the computational amount but not for shortening the length of parameters in order to save memory space. Consequently, there is no teaching in Miyaji regarding how the parameter "c" is to be selected so as to significantly reduce the length of the parameters in the second form. Miyaji only proposes setting "a = 0" or "a = -3" in order to reduce the computation amount (see page 3, last three lines above Table 1). Therefore, the invention of the instant application should not have been obvious to a person having ordinary skills in the art and having knowledge of Miyaji.

Regarding the article by Menezes entitled "Elliptic Curve

Public Key Cryptosystems" (we believe the title was incorrectly quoted by the examiner), the first form of the elliptic curve is found on page 100. On page 99, notes are given describing the efforts made to reduce the cost of hardware implementations by choosing a method that does not require the storage of intermediate results. A short mention is made on the same page of methods for selecting elliptic curves over prime fields that are suitable for implementing Schnorr's digital signature scheme on smart cards. It should be noted, that the pages cited by the examiner fall under the subsection 9.9 "Notes" and refer to external literature without giving details relevant to the invention.

In contrast to the invention of the instant application the second form of the elliptic curve is not mentioned at all in Menezes, and Menezes does not describe the transformation of the first form into the second form. More importantly, like in Miyaji, no hint is given to select the parameters of the transformation so that at least the length of a second parameter is shortened in comparison with the first parameter. Furthermore, no information on how the parameters are to be chosen is given.

Independent claims 1, 9 and 12 of the instant application recite that "parameter a is shortened by selecting the constant c such that ... ". Since neither Menezes nor Mijaki teach this step or feature, claims 1, 9 and 12 are believed to be allowable.

It is accordingly believed to be clear that none of the references, whether taken alone or in any combination, either show or suggest the features of claims 1, 9 or 12. Claims 1, 9 and 12 are, therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claim 1, 9 or 12.

In view of the foregoing, reconsideration and allowance of claims 1-13 are solicited.

If an extension of time is required, petition for extension is herewith made. Any extension fee associated therewith should be charged to the Deposit Account of Lerner and Greenberg, P.A., No. 12-1099.

Please charge any other fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner and Greenberg, P.A., No. 12-1099.

Respectfully submitted,

For Applicants

REL:cgm

RALPH E. LOCHER
REG. NO. 41,947

January 31, 2005

Lerner and Greenberg, P.A.
P.O. Box 2480
Hollywood, Florida 33022-2480
Tel.: (954) 925-1100
Fax: (954) 925-1101